MACHINE LEARNING–GENETIC ALGORITHM BASED OPTIMIZATION OF NETWORK BEHAVIOUR

N. Akhila
Research Scholar
University of Technology
Jaipur.

Dr. Suneel Pappala
Research Supervisor
University of Technology
Jaipur.

Dr. Rama Sree
Research Co-Supervisor
University of Technology
Jaipur.

ABSTRACT

Machine learning (ML) promises advances in automation and threat detection for the future generations of communication networks. However, new threats are introduced, as adversaries target ML systems with malicious data. Adversarial attacks on tree-based ML models involve crafting input perturbations that exploit non-smooth decision boundaries, causing misclassifications. These so-called evasion attacks are imperceptible, as they do not significantly alter the input data distribution and have been shown to degrade the performance of tree-based models across various tasks. Adversarial training and genetic algorithms have been proposed as potential defenses against these attacks. This study evaluates an optimization approach inspired by genetic algorithms to generate adversarial samples and studies the impact of adversarial training on the accuracy of attack detection. AI is useful in many different disciplines. One type of AI application is a neural network; task specific AI consists of many different architecture types. Genetic algorithm optimization, a population-based evolutionary algorithm, is proposed to help find the most efficient neural network architecture for a specific task.

Keywords: *Machine learning (ML), genetic algorithms, neural network, Genetic algorithm optimization, neural network architecture, AI application.*

INTRODUCTION

Heuristic search is made easier using genetic algorithms. Applying GAs to machine learning is a controversial topic. Using chess as an example, the following study explores and explains the point. Following an overview of machine learning, the first part defined classifier systems and discussed their many kinds. A short review of genetic algorithms follows. Section IV described the use of GAs in machine learning using chess as an example. If the rules can be given the right fitness values, GA's provide an effective solution when there are numerous rules to apply for a certain situation. There is a growing need for simple, intelligent solutions in our fast-paced environment. Many have speculated for a long time that AI would eventually become an integral part of our life. Reason being, AI has sparked moral and philosophical discussions, with some seeing it as a game-changing technology and others as a sign of the end of an era. In order to include human labor, industry is also being pushed to seek out more advanced technology by both customer needs and the falling cost of smart equipment. In contrast to our earlier perceptions, the future now seems to be becoming closer. Following a computer's 2015 defeat of the world Go champion, electric vehicle manufacturer Tesla poured resources into R&D to create smarter, more autonomous vehicles, solidifying their position as market leaders. As reports of autonomous cars and humanoid robots proliferate, the general population perceives the impending transformation as imminent. Machines still have a ways to go before they can do things like walking, finding their way around in very unpredictable surroundings, and solving issues that need reasoning when faced with ambiguity. In order to discover a hybrid solution that addresses the limitations of each method and yields competitive results while also providing innovative approaches to improve the exploration work, this project will merge three separate empirical investigations.

LITERATURE REVIEW

Mikael Salovaara, (2023) since there are many different materials, exposure circumstances, and performance criteria. Hygrothermal models, which assess an object's resilience in response to moisture exposure, are quite intricate and need a great deal of knowledge to implement correctly. In the event that ML considerably streamlines the design process, hygrothermal simulations could be unnecessary. Machine learning made the design process easier and made the structure more water resistant. Machine learning-based methods for predicting mold index and maximum moisture content could be useful during the building of new home walls. The results demonstrate that ML outperforms hygrothermal models ($R2 > 0.90$) in forecasting performance within the structure's restrictions, including exposure circumstances. Performance is inversely proportional to material properties of the vapor barrier and continuous insulating layer, according to the data.

Radha Raman Chandan (2022) genetic algorithms address optimization problems by using evolutionary principles. These approaches include mutation, miscellaneous, intersect, and bequest, among others. Actually, it refers to a competent, concurrent, and globally search strategy that continuously builds data on the search space and the CM search space to adapt to the ideal search result. Generating a large number of candidate items and comparing them to the whole database is the traditional way for mining multilevel association rules. Nevertheless, because to the high processing expenses involved, the majority of mining activities are worthless. The inherited algorithms provide a novel approach to handling such problems.

Xuewen Xia (2022) asserts that cloud computing is becoming more significant in several real-world domains. Therefore, it is becoming more important to resolve workflow scheduling concerns, such as how to allocate and schedule resources in a cloud computing setting. On lower scales, evolutionary algorithms (EAs) function well for scheduling challenges, but when applied to larger-scale workflow applications, their limitations become apparent. This study takes on the problem of optimizing workflow scheduling by using a MOGA, or multi-objective genetic algorithm. Findings from this research point to an initiation scheduling sequence as a means to improve search efficiency. When the virtual machine (VM) for each job is being initialized, this approach takes the data amount into account. As long as the basic scheduling method is followed appropriately, this study will achieve its goals of making energy use optimization and makespan optimization. During the early stages of evolution, the population is kept exploring by using standard operators like as mutation and crossover.

Martin Sagayam (2021) there are several conceivable indications of cancer due to the disease's multi-subtype nature. Cancer fact-finding initiatives have mostly focused on early diagnosis and cancer type prediction since they might lead to better therapeutic care for cancer survivors. Due to the requirement of risk categorization for cancer patients, many scientists in the domains of genetics and biosciences have explored the possibilities of ML algorithms for cancer diagnosis and therapy. Using these tools, we have been able to model the development and treatment of cancer in humans. Another proof of machine learning algorithms' importance is their capacity to extract valuable information from datasets that would otherwise be unavailable. A variety of methods, such as artificial neural networks and Bayesian networks, are part of this set of resources. The precision and dependability of prediction models constructed using Decision Trees and Support Vector Machines are greatly relied upon by the cancer research community. Here we take a look at the present landscape of cancer development modeling using machine learning techniques.

Lu Lu (2021) numerically discretizing PDEs for application in simulations of multiphysics problems has made significant strides in recent years. However, difficulties like mesh fabrication difficulty and high-dimensional problem instabilities managed by parameterized PDEs are still there. Due of the large number of formulations and complex computer codes typically required, using hidden physics to solve inverse issues may also be costly. Machine learning has emerged as a viable option; yet, when it comes to scientific concerns, big datasets aren't always accessible for training deep neural networks. Another option for training these networks would be to collect data at random locations in the continuous space-time domain, in accordance with physical laws. This physics-based learning uses neural networks or other kernel-based regression networks to include mathematical models with (noisy) data. Specialist network topologies that intrinsically fit certain physical invariants may be built to further enhance accuracy, training speed, and generalizability. We will go over the latest innovations in physics-informed machine learning, drawing attention to its pros and cons and its many forward and inverse uses, such as solving high-dimensional problems and uncovering hidden physics.

Machine Learning

Creating algorithms that can enhance computer behavior via the analysis of real-world data is the primary objective of machine learning. Machine learning gives computers the ability to learn new things. For students just starting out with probability distributions, examples could help clarify and cement key points. Observing the instances, one may discern the connection between input and output. Discovering ways to train computers to recognize and interpret complex patterns and draw smart conclusions from relatively basic instances is a primary objective of machine learning. Given every conceivable input, it is impossible to record every conceivable action in a collection of observable instances. Students, in order to thrive in unfamiliar settings, must have the big picture in mind as they examine the provided instances. We assert that an algorithm has gained knowledge from experience E when its performance, as measured by P, improves over time for tasks belonging to a certain class T. Teaching students to draw conclusions about the world based on their own experiences is education's principal goal.

Types of Machine Learning Algorithms

Machine learning algorithms may be categorized according to the intended output of the algorithm. There are two categories: monitored and unsupervised. Supervised learning produces a function that correlates inputs with intended outcomes. For instance, with MS Word, the conversion of voice to text is feasible. A text is extracted, and training is administered to the system, namely the computer, to acquire the pronunciation and nuances of the speaker. Unsupervised learning analyzes a collection of inputs, such as clustering. Additional algorithms are derived from the aforementioned two, as detailed in the subsequent section. Semi-supervised learning integrates both supervised and unsupervised methods to develop a classifier. Reinforcement learning determines optimal actions in certain situations within a given context. Every action influences the environment, which in turn offers feedback via rewards and penalties. Transduction aims to forecast novel outputs based on training inputs. Learning to learn develops its own inductive bias based on prior occurrences.

Types Of Selection Styles Available

Methods for selecting events, using a roulette wheel, and ranking candidates according to predetermined standards. To solve optimization problems, heuristic search methods like genetic algorithms are used. Computing uses it as part of a subset of evolutionary algorithms. To solve optimization problems, genetic algorithms use natural selection and genetic principles.

Learning in Neural Networks

Neural networks are used for supervised learning in Reinforcement Learning. In this setting, training the model's parameters—including FFNN weights—to learn a desired mapping is the objective.

The training technique takes a set of datapoints encoded as tuples (xi, yi) as input and uses them to gain this mapping. A label yi is assigned to each input sample xi in supervised learning. Labels yi, which are learned from a collection of training points xi to a target mapping $f_o(x)$, are often noisy approximations of the values of $f_o(xi)$. Given that this is the anticipated behavior, the training instances instruct the output layer to provide a value close to $f_o(xi)$. To get a fair estimate of f_o, the learning system should instead determine how to use these layers most efficiently. The reason these intermediary layers are referred to as hidden is because the training data does not explicitly define how they are expected to behave.

Big Data

The concept of Big Data has been expanding rapidly over the last 20 years, becoming increasingly applicable to improving operational and corporate efficiency. Nevertheless, uncertainty and misunderstanding persist due to the lack of a globally accepted meaning of the word. Contrarily, extensive bibliographic study on Big Data from 2011–2015 established that it originated in the mid–1990s. Big Data and its characteristics may have varying meanings depending on the industry and the specific technology used. Organizational and commercial context, data collection quantity, analytical challenge, and available technology for handling and processing massive data sets are some of the variables that influence how Big Data is characterized. According to the academic community, "Big Data is a collection of data with complexity, diversity, heterogeneity, and high potential value that are difficult to process and analyze in reasonable time." Companies use the following phrase: "Big Data is a new type of strategic resource in the digital era and the key factor to drive innovation, which is changing the way of humans' current production and living." That is how it is defined in academia.

Hybrid Genetic and Reinforcement Learning

Machine learning Finally, a review of the literature on works aiming to merge RL with Genetic Algorithms is provided in the similar work section. These algorithms often use Genetic Algorithms to enhance the RL process.

Using a Genetic Algorithm, the best hyperparameters for RL training are found. In our quest to develop more cooperative algorithms, we suggest hybrid systems that augment neural-Q function training with GA. It uses NEATS to update the network's architecture in real-time, even if just the weights change.

To train the remaining network synaptic weights using gradient approaches, a typical RL algorithm is used. However, separate training was conducted for the GA and Gate weights. These Gates, which are analogous to the dropout layers in conventional NNs, act as regularizers. Regularization is a collection of techniques that aims to fight overfitting by lowering co-adaptation; NN, with its reputation for generalizability, benefits substantially from this approach. Deep Neural Networks replicate complicated activities by learning to extract useful information by training each layer to handle input effectively.

RESEARCH METHODOLOGY

Researchers in the field of machine learning have relied on GAs for a long time because of their usefulness as general-purpose optimizers. This section provides further analysis and dives deeper into the works that are relevant to the thesis. Upcoming studies will conduct in-depth analyses of two cutting-edge RL and GA algorithms. The discipline of Evolutionary Robotics was officially formed in a fundamental article published in the late 90s. In this field, researchers work on creating neural principles that GA may utilize to teach robots to do certain tasks. At the time, Reinforcement Learning's application to complex systems like robots was in its early stages. Obstacles included insufficient time for training and an absence of sturdy equipment. Instead of learning to maximize regardless of how broad the formulation is. This is one of the key reasons the region has such an influence, according to ER academics. While Evolutionary Robotics successfully tackles some issues with GAs and simulation-based ML, it falls short when it comes to tackling the primary drawback of GAs—their inability to generalize in stochastic situations—in complex and realistic scenarios. In the last section, we take a high-level look at the GA/RL hybrid approaches that have been suggested. Despite the abundance of research on the subject, this study stands out by comparing algorithms to get a deeper understanding of distributed exploration. It delves into the algorithm that most closely resembles traditional distributed RL approaches, offering a fresh perspective.

RESULTS AND DISCUSSIONS

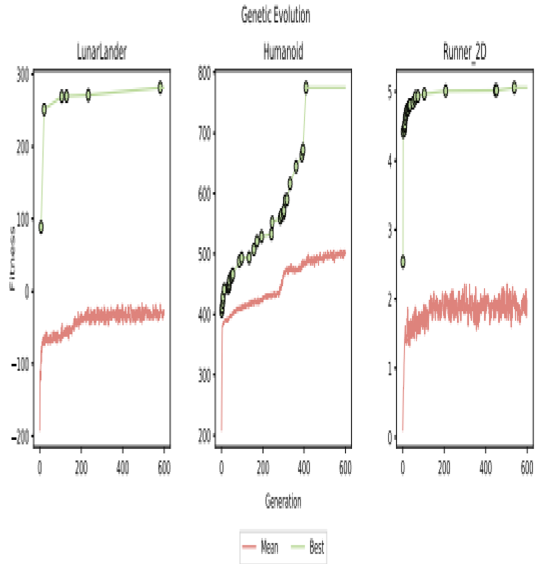
Among the issues raised, this one has the most randomness, in my opinion. An episode's fitness is the total distance traveled from the beginning to the finish, along the local surge axis of the robot, which is lowered exponentially with the number of collisions reported.

Table 1: AFPO Neural Evolution

AFPO Parameters	
Parameter	Value
Population Size	100
Children Size	200
Elite %	10%
Immigrant %	0.5%
Crossover K	2
AFPO K	2
Generations	600

Genome Network Parameters	
Parameter	Value
Layer_1 Size	400
Layer_2 Size	300
Activation	ReLU
Normalization	LayerNorm

The neural policy architecture adheres to the original DDPG algorithm. The total fitness of each person is the average fitness over five distinct events. Graph 1 illustrates the average and optimal fitness of the population throughout the evolutionary process.

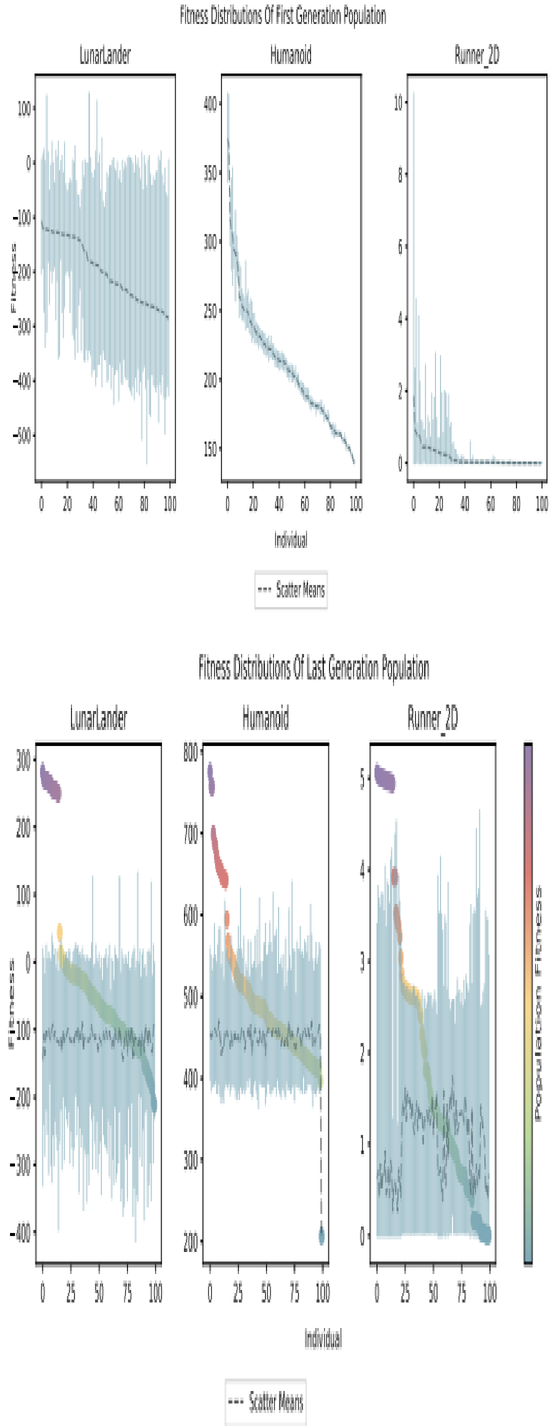


Graph 1: Average and Optimal Fitnesses Throughout Evolution

Each person's fitness is defined as the sum of their fitness scores across all episodes, and the empirical mean and variance of all fifty episodes constitute their fitness dispersion.

We specifically monitor the fitness distributions of three groups of individuals:

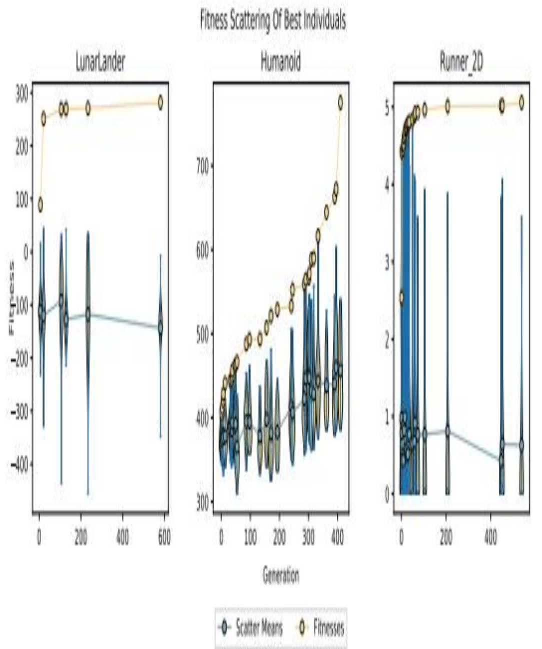
Commencement: we calculate the Fitness Scattering for each member of the initialized population, including 100 people. Graph 2.



Graph 2: Estimated Fitness Distributions of Initial Population

End: we calculate the Fitness Scattering for each individual in the final population, at generation 600, including 100 individuals. Graph 3

Bests: when an individual surpasses the present optimal population fitness, we calculate its Fitness Scattering.



Graph 3: With Genetic Finesses

The study meat is found in results, which are very important; nonetheless, findings 1 may have been expected. Graph 3 shows the evolution of the top individuals' fitness distribution in the third scenario. In stochastic contexts, the fitness metric clearly outweighs the real expected return value. The diversity of these results really stays consistent as learning advances, too. It is clear from identifying more efficient when evaluated against the fitness and robustness predictions, the policies do not improve at all. Rather, similar high-variance score distributions may have their top values sampled to find fitnesses that increase with time.

CONCLUSIONS

This research aimed to combine genetic algorithms (GA) with machine learning (ML) to improve network performance in areas including efficiency, scalability, security, and adaptability. More and more devices are going online, which means real-time performance is more important than ever. However, conventional rule-based systems are struggling to keep up with the ever-changing network conditions. It seems that a convincing strategy to enhance network behavior in this case would be to combine the optimization capability of evolutionary algorithms with the adaptive and predictive skills of ML. The results of our research show that classification algorithms, deep reinforcement learning, clustering approaches, and other machine learning techniques can control bandwidth, balance network loads, and identify intrusions. Trends, behavior, and intelligent judgments may all be found using these methods. While Decision Trees and Support Vector Machines performed well for traffic categorization and anomaly detection, supervised learning models such as DBSCAN and K-means assisted in identifying network behavior for better policy choices. Complex problems involving numerous variables and constraints include scheduling, resource allocation, and routing pathways. To overcome these challenges, the evolutionary approach offered a firm foundation. Network strategies have been continuously improved by the development of better solutions over generations, thanks to natural selection, which is inspired by biological processes.

REFERENCES

1. *Lu Lu (2021), "Physics-informed machine learning", Nature Reviews Physics, ISSNno:2522-5820, DOI:10.1038/s42254-021-00314-5*
2. *Mikael Salonvaara (2023), ""Application of Machine Learning to Assist a Moisture Durability Tool", Energies, ISSNno:1996-1073, Vol.16(4), Pages.1-20.*

3. *Radha Raman Chandan (2022), "Genetic Algorithm and Machine Learning", Advanced Bioinspiration Methods for Healthcare Standards, Policies, and Reform, ISBNno:9781668456569, Pages.167-182.DOI:10.4018/978-1-6684-56 56-9.ch009*
4. *Xuewen Xia (2022), "Multi-objective workflow scheduling based on genetic algorithm in cloud environment", Information Sciences, ISSNno:1872-6291, Vol.606, Pages.38-59. https://doi.org/10.1016/j.ins.2022.05.053*
5. *Martin Sagayam (2021), "Machine Learning Frameworks in Cancer Detection", E3S Web of Conferences, ISSNno:2267-1242, Vol.297(2), Pages. 01073. DOI:10.1051/e3sconf/202129701073*
6. *Sabyasachi Pramanik (2014), "Image Steganography Using Wavelet Transform and Genetic Algorithm", International Journal of Innovative Research in Advanced Engineering (IJIRAE), ISSNno:2349-2163, Vol.1, Issue.1,*
7. *Surbhi Bhatia (2011), "Application of Genetic Algorithms in Machine learning", International Journal of Computer Science and Information Technologies, ISSNno:0975-9646, Vol.2(5), Pages.2412-2415.*
8. *Mario Pavone (2024), "Machine Learning and Genetic Algorithms: A case study on image reconstruction", Knowledge-Based Systems, ISSNno:1872-7409, Vol.284, Pages.111194. https://doi.org/10.1016/j.knosys.2023.111194*
9. *Patrick Meyer (2022), "Machine learning at the service of meta-heuristics for solving combinatorial optimization problems: A state-of-the-art", European Journal of Operational Research, ISSNno:1872-6860, Vol.296, Issue.2, Pages. 393-422. https://doi.org/10.1016/j.ejor.2021.04.032*
10. *Alice E. Smith (2006), "Multi-objective optimization using genetic algorithms: A tutorial", Reliability Engineering & System Safety, ISSN no: 0951-8320, Vol.91, Issue.9, Pages.992-1007. https://doi.org/10.1016/j.ress.20 05.11.018*